Amendments to the Claims:

1-30. (Cancelled)

31. (Currently amended) A system for protecting a distributed network from unauthorized access, the system comprising:

[[an]] first and second intrusion detection ~~system~~ systems, respectively including:

[[an]] first and second intrusion detection ~~module~~ modules, and

[[a]] first and second communications management ~~module~~ modules respectively coupled to the first and second intrusion detection ~~module~~ modules; and

an intrusion analysis system coupled to the first and second intrusion detection ~~system~~ systems, and including:

an intrusion analysis module, and

an intrusion reaction coordination module coupled to the intrusion analysis module,

wherein the first intrusion detection module detects a respective possible unauthorized access attempt into ~~or within~~ a distributed network being protected,

the second intrusion detection module detects a respective possible unauthorized access attempt within the distributed network being protected,

the first and second communications management ~~module is~~ modules are coupled to the intrusion analysis module and ~~forwards~~ forward to the intrusion analysis module respective information regarding the respective detected possible unauthorized access attempt,

the intrusion analysis module determines based on the respective information regarding the respective detected possible unauthorized access attempt whether or not the respective detected possible unauthorized access attempt is authorized,

if the intrusion analysis module determines that the respective detected possible unauthorized access attempt is authorized, the intrusion analysis module respectively forwards, via the first and second communications management ~~module~~ modules, respective information to the first and second intrusion detection ~~module~~ modules that the respective possible unauthorized access attempt is authorized, and

if the intrusion analysis module determines that the respective detected possible unauthorized access attempt is not authorized, the intrusion analysis module determines, via the intrusion reaction coordination module, appropriate actions, including (i) forwarding respective information regarding the respective detected unauthorized access attempt into the distributed network being protected to a monitoring center external to the distributed network being protected, and processing respective information from the monitoring center regarding the respective detected unauthorized access attempt into the distributed network being protected, (ii) forwarding respective information regarding the respective detected unauthorized access attempt within the distributed network being protected for handling internally within the distributed network being protected, and processing respective information for internally handling the respective detected unauthorized access attempt within the distributed network being protected, and (iii) forwarding respective information regarding the respective detected unauthorized access attempt within the distributed network being protected to the monitoring center external to the distributed network being protected, and processing respective information from the monitoring center regarding the respective detected unauthorized access attempt within the distributed network being protected,

wherein the intrusion analysis system in cooperation with the first and second intrusion detection ~~system~~ systems enable communications between the monitoring center and an entity attempting the respective unauthorized access attempt without the entity being made aware that the entity attempting the respective unauthorized access attempt is communicating with the monitoring center,

wherein the monitoring center sends information to the analysis system and intended for the entity attempting the unauthorized access attempt, the analysis system substitutes origin information of the monitoring center from the received information with origin information of a target of the respective unauthorized access attempt and forwards the substituted information to the entity attempting the respective unauthorized access attempt, whereby it appears to the entity attempting the respective unauthorized access attempt that communications are continuing with the target of the respective unauthorized access attempt, and

wherein the intrusion analysis system in cooperation with the first intrusion detection system engages the entity attempting the respective unauthorized access attempt to determine the location or origin of the entity attempting the respective unauthorized access attempt.

32. (Cancelled)

33. (Previously presented) The system of claim 31, wherein the intrusion analysis system communicates with monitoring center via a secure tunnel.

34. (Currently amended) The system of claim 31, wherein the respective communications from the monitoring center to the entity attempting the respective unauthorized access attempt are modified, via the intrusion analysis system and the respective first and second intrusion detection ~~system~~ systems, to appear as if the communications originate from the distributed network being protected.

35. (Currently amended) The system of claim 31, wherein the intrusion analysis system logs respective information regarding communications with the entity attempting the respective unauthorized access attempt.

36-37. (Cancelled)

38. (Currently amended) The system of claim 31, wherein the first and second intrusion detection ~~module detects~~ modules respectively detect whether or not the respective possible unauthorized access attempt into or within the distributed network being protected is internal or external to the network being protected.

39. (Currently amended) The system of claim 31, wherein if second intrusion detection module detects that the possible respective unauthorized access attempt is internal to the network being protected, the second intrusion detection module forwards via the second communications management module respective information regarding the possible internal unauthorized access attempt to the intrusion analysis module, and the intrusion

analysis module evaluates the received information and if the intrusion analysis module determines that the possible internal unauthorized access attempt is not authorized, the intrusion analysis module determines whether or not a retaliatory action should be taken, including handling the unauthorized access attempt internally or providing information to the monitoring center regarding the unauthorized access attempt.

40. (Previously presented) The system of claim 31, wherein the monitoring center comprises a law enforcement entity.

41. (Currently amended) The system of claim 31, further comprising a database,

wherein the intrusion analysis module employs the database, including respective information regarding previous respective unauthorized access attempts, to determine whether or not the respective detected possible unauthorized access attempt is authorized.

42. (Currently amended) The system of claim 41, wherein the database includes respective profiles of information related to one or more entities associated with the respective previous unauthorized access attempts, including origin information regarding the respective previous unauthorized access attempts.

43. (Currently amended) The system of claim 41, wherein the intrusion analysis module is configured to query the database to determine whether or not the respective possible unauthorized access attempt is an error in communications, including a bit error.

44. (Currently amended) The system of claim 31, wherein the intrusion analysis module is configured to determine based on respective historical profiles, and respective previous unauthorized access attempts whether or not the detected respective possible unauthorized access attempt is authorized.

45. (Currently amended) The system of claim 31, wherein the intrusion reaction coordination module determines the respective appropriate actions based on a number of respective previous unauthorized access attempts, and a nature of the respective unauthorized

access attempt, including destructiveness of packets received during the respective unauthorized access attempt.

46. (Currently amended) The system of claim 31, wherein the intrusion reaction coordination module, to determine the respective appropriate actions, analyzes the respective information received by the first and second intrusion detection ~~module~~ modules, respective historical information regarding respective unauthorized access attempts, respective source and destination ports of respective unauthorized access attempts, respective IP address information of respective unauthorized access attempts, and respective information received from a central repository that catalogs respective information related to respective unauthorized access attempts from one or more other protected networks.

47. (Currently amended) The system of claim 46, wherein the intrusion detection analysis is based on at least one of a look-up table, a neural network analysis, and a predetermined event sequence.

48. (Currently amended) The system of claim 31, wherein if the intrusion reaction coordination module determines that a responsive or retaliatory action is not required, the intrusion reaction coordination module respectively instructs the first and second intrusion detection ~~module~~ modules to block communications from an entity attempting the respective unauthorized access attempt.

49. (Currently amended) The system of claim 31, wherein if the intrusion reaction coordination module determines that a responsive or retaliatory action is not required, the intrusion reaction coordination module respectively instructs the first and second intrusion detection ~~module~~ modules to block communications from an entity that matches one or more characteristics of the respective unauthorized access attempt.

50. (Currently amended) The system of claim 41, wherein the intrusion reaction coordination module logs respective information regarding an entity attempting the respective

unauthorized access attempt to the database for use in a future unauthorized access attempt by the entity.

51. (Currently amended) The system of claim 31, wherein the intrusion analysis module ~~system~~ is configured to store information regarding an address to which the respective unauthorized access attempt was directed for use by the intrusion reaction coordination module to determine the respective appropriate actions.

52. (Currently amended) The system of claim 41, wherein upon receipt of a respective communication from the monitoring center, the first and second intrusion detection ~~system~~ systems in cooperation with the intrusion analysis system analyze the respective communication, determine address information of a source of the respective communication from the monitoring center, and ~~removes~~ remove the address information from the respective communication from the monitoring center leaving the remaining information for further analysis.

53. (Previously presented) The system of claim 52, wherein the address information of the source of the communication from the monitoring center is stored in the database, and the intrusion analysis module is configured to use the address information to communicate information to the monitoring center, including information regarding a response to a password request by an entity attempting the unauthorized access attempt.

54. (Currently amended) The system of claim 31, wherein the first and second intrusion detection ~~system~~ systems in cooperation with the intrusion analysis system conceal an identity of the monitoring center, communicate respective information with the monitoring center, and screen respective underlying content in the communicated information, including removing sensitive information from the communicated information.

55. (Currently amended) The system of claim 54, wherein the first and second intrusion detection ~~system~~ systems in cooperation with the intrusion analysis system employ a policy file to regulate the screening and removing of the sensitive information, including

removing all content or core information, removing content having certain words, and removing content originating from a predetermined location.

56. (Currently amended) The system of claim 31, wherein the first and second intrusion detection ~~system~~ systems and the intrusion analysis system cooperate with the monitoring center to aid in detecting a source of the respective unauthorized access attempt.

57. (Currently amended) The system of claim 56, wherein the first and second intrusion detection ~~system~~ systems in cooperation with the intrusion analysis system receive from the monitoring center respective information regarding unauthorized accesses or access attempts into or within distributed networks.

58. (Currently amended) The system of claim 57, wherein the first and second intrusion detection ~~system~~ systems in cooperation with the intrusion analysis system analyze the respective information regarding unauthorized accesses or access attempts into or within the distributed networks received from the monitoring center to determine if the respective received information matches a profile or has characteristics corresponding to one or more respective known unauthorized access attempts.

59. (Currently amended) The system of claim 58, wherein, upon detection of an unauthorized access attempt, the first and second intrusion detection ~~system~~ systems in cooperation with the intrusion analysis system forward information regarding the respective unauthorized access attempt to the monitoring center for inclusion in a central database that maintains the information regarding the respective unauthorized accesses or access attempts into or within the distributed networks.

60. (Previously presented) The system of claim 31, wherein the system is implemented with one or more hardware and or software components.

61. (Currently amended) A method for protecting a distributed network from unauthorized access for use in a system including [[an]] first and second intrusion detection

~~system~~ systems respectively having [[an]] first and second intrusion detection ~~module~~ modules, and [[a]] first and second communications management ~~module~~ modules coupled to the first and second intrusion detection ~~module~~ modules, and intrusion analysis system coupled to the first and second intrusion detection ~~system~~ systems, and including an intrusion analysis module, and an intrusion reaction coordination module coupled to the intrusion analysis module, the method comprising:

detecting, by the first intrusion detection module, a respective possible unauthorized access attempt into ~~or within~~ a distributed network being protected;

detecting, by the second intrusion detection module, a respective possible unauthorized access attempt within the distributed network being protected;

forwarding, by the first and second communications management modules, respective information regarding the respective detected possible unauthorized access attempt to the intrusion analysis module;

determining, by the intrusion analysis module, based on the respective information regarding the respective detected possible unauthorized access attempt whether or not the respective detected possible unauthorized access attempt is authorized;

if the intrusion analysis module determines that the respective detected possible unauthorized access attempt is authorized, respectively forwarding, by the intrusion analysis module, via the first and second communications management modules, respective information to the first and second intrusion detection ~~module~~ modules that the respective possible unauthorized access attempt is authorized, and

if the intrusion analysis module determines that the respective detected possible unauthorized access attempt is not authorized, determining, by the intrusion analysis module, via the intrusion reaction coordination module, appropriate actions, including (i) forwarding respective information regarding the respective detected unauthorized access attempt into the distributed network being protected to a monitoring center external to the distributed network being protected, and processing respective information from the monitoring center regarding the respective detected unauthorized access attempt into the distributed network being protected, (ii) forwarding respective information regarding the respective detected unauthorized access attempt within the distributed network being protected for handling internally within the distributed network being protected, and processing respective

information for internally handling the respective detected unauthorized access attempt within the distributed network being protected, and (iii) forwarding respective information regarding the respective detected unauthorized access attempt within the distributed network being protected to the monitoring center external to the distributed network being protected, and processing respective information from the monitoring center regarding the respective detected unauthorized access attempt within the distributed network being protected,

wherein the intrusion analysis system in cooperation with the first and second intrusion detection ~~system~~ systems enable communications between the monitoring center and an entity attempting the respective unauthorized access attempt without the entity being made aware that the entity attempting the respective unauthorized access attempt is communicating with the monitoring center,

wherein the monitoring center sends information to the analysis system and intended for the entity attempting the unauthorized access attempt, the analysis system substitutes origin information of the monitoring center from the received information with origin information of a target of the respective unauthorized access attempt and forwards the substituted information to the entity attempting the respective unauthorized access attempt, whereby it appears to the entity attempting the respective unauthorized access attempt that communications are continuing with the target of the respective unauthorized access attempt, and

wherein the intrusion analysis system in cooperation with the first intrusion detection system engages the entity attempting the respective unauthorized access attempt to determine the location or origin of the entity attempting the respective unauthorized access attempt.

62. (Cancelled)

63. (Currently amended) The method of claim 61, wherein the intrusion analysis system communicates with monitoring center via a secure tunnel.

64. (Currently amended) The method of claim 61, wherein the respective communications from the monitoring center to the entity attempting the respective unauthorized access attempt are modified, via the intrusion analysis system and the respective

first and second intrusion detection ~~system~~ systems, to appear as if the communications originate from the distributed network being protected.

65. (Currently amended) The method of claim 61, wherein the intrusion analysis system logs respective information regarding communications with the entity attempting the respective unauthorized access attempt.

66-67. (Cancelled)

68. (Currently amended) The method of claim 61, wherein the first and second intrusion detection ~~module detects~~ modules respectively detect whether or not the respective possible unauthorized access attempt into or within the distributed network being protected is internal or external to the network being protected.

69. (Currently amended) The method of claim 61, wherein if second intrusion detection module detects that the possible respective unauthorized access attempt is internal to the network being protected, the second intrusion detection module forwards via the second communications management module respective information regarding the possible internal unauthorized access attempt to the intrusion analysis module, and the intrusion analysis module evaluates the received information and if the intrusion analysis module determines that the possible internal unauthorized access attempt is not authorized, the intrusion analysis module determines whether or not a retaliatory action should be taken, including handling the unauthorized access attempt internally or providing information to the monitoring center regarding the unauthorized access attempt.

70. (Previously presented) The method of claim 61, wherein the monitoring center comprises a law enforcement entity.

71. (Currently amended) The method of claim 61, the system further comprising a database,

wherein the intrusion analysis module employs the database, including respective information regarding previous respective unauthorized access attempts, to determine whether or not the respective detected possible unauthorized access attempt is authorized.

72. (Currently amended) The method of claim 71, wherein the database includes respective profiles of information related to one or more entities associated with the respective previous unauthorized access attempts, including origin information regarding the respective previous unauthorized access attempts.

73. (Currently amended) The method of claim 71, wherein the intrusion analysis module is configured to query the database to determine whether or not the respective possible unauthorized access attempt is an error in communications, including a bit error.

74. (Currently amended) The method of claim 61, wherein the intrusion analysis module is configured to determine based on respective historical profiles, and respective previous unauthorized access attempts whether or not the detected respective possible unauthorized access attempt is authorized.

75. (Currently amended) The method of claim 61, The system of claim 31, wherein the intrusion reaction coordination module determines the respective appropriate actions based on a number of respective previous unauthorized access attempts, and a nature of the respective unauthorized access attempt, including destructiveness of packets received during the respective unauthorized access attempt.

76. (Currently amended) The method of claim 61, wherein the intrusion reaction coordination module, to determine the respective appropriate actions, analyzes the respective information received by the first and second intrusion detection ~~module~~ modules, respective historical information regarding respective unauthorized access attempts, respective source and destination ports of respective unauthorized access attempts, respective IP address information of respective unauthorized access attempts, and respective information received

from a central repository that catalogs respective information related to respective unauthorized access attempts from one or more other protected networks.

77. (Currently amended) The method of claim 76, wherein the intrusion detection analysis is based on at least one of a look-up table, a neural network analysis, and a predetermined event sequence.

78. (Currently amended) The method of claim 61, wherein if the intrusion reaction coordination module determines that a responsive or retaliatory action is not required, the intrusion reaction coordination module respectively instructs the first and second intrusion detection ~~module~~ modules to block communications from an entity attempting the respective unauthorized access attempt.

79. (Currently amended) The method of claim 61, wherein if the intrusion reaction coordination module determines that a responsive or retaliatory action is not required, the intrusion reaction coordination module respectively instructs the first and second intrusion detection ~~module~~ modules to block communications from an entity that matches one or more characteristics of the respective unauthorized access attempt.

80. (Currently amended) The method of claim 71, wherein the intrusion reaction coordination module logs respective information regarding an entity attempting the respective unauthorized access attempt to the database for use in a future unauthorized access attempt by the entity.

81. (Currently amended) The method of claim 61, wherein the intrusion analysis module ~~system~~ is configured to store information regarding an address to which the respective unauthorized access attempt was directed for use by the intrusion reaction coordination module to determine the respective appropriate actions.

82. (Currently amended) The method of claim 71, wherein upon receipt of a respective communication from the monitoring center, the first and second intrusion detection

~~system~~ systems in cooperation with the intrusion analysis system analyze the respective communication, determine address information of a source of the respective communication from the monitoring center, and ~~removes~~ remove the address information from the respective communication from the monitoring center leaving the remaining information for further analysis.

83. (Previously presented) The method of claim 82, wherein the address information of the source of the communication from the monitoring center is stored in the database, and the intrusion analysis module is configured to use the address information to communicate information to the monitoring center, including information regarding a response to a password request by an entity attempting the unauthorized access attempt.

84. (Currently amended) The method of claim 61, wherein the first and second intrusion detection ~~system~~ systems in cooperation with the intrusion analysis system conceal an identity of the monitoring center, communicate respective information with the monitoring center, and screen respective underlying content in the communicated information, including removing sensitive information from the communicated information.

85. (Currently amended) The method of claim 84, wherein the first and second intrusion detection ~~system~~ systems in cooperation with the intrusion analysis system employ a policy file to regulate the screening and removing of the sensitive information, including removing all content or core information, removing content having certain words, and removing content originating from a predetermined location.

86. (Currently amended) The method of claim 61, wherein the first and second intrusion detection ~~system~~ systems and the intrusion analysis system cooperate with the monitoring center to aid in detecting a source of the respective unauthorized access attempt.

87. (Currently amended) The method of claim 86, wherein the first and second intrusion detection ~~system~~ systems in cooperation with the intrusion analysis system receive

from the monitoring center respective information regarding unauthorized accesses or access attempts into or within distributed networks.

88. (Currently amended) The method of claim 87, wherein the first and second intrusion detection ~~system~~ systems in cooperation with the intrusion analysis system analyze the respective information regarding unauthorized accesses or access attempts into or within the distributed networks received from the monitoring center to determine if the respective received information matches a profile or has characteristics corresponding to one or more respective known unauthorized access attempts.

89. (Currently amended) The method of claim 88, wherein, upon detection of an unauthorized access attempt, the first and second intrusion detection ~~system~~ systems in cooperation with the intrusion analysis system forward information regarding the respective unauthorized access attempt to the monitoring center for inclusion in a central database that maintains the information regarding the respective unauthorized accesses or access attempts into or within the distributed networks.

90. (Previously presented) The method of claim 61, wherein said method is implemented with one or more hardware and/or software devices configured to perform the steps of the method.

91. (Previously presented) The method of claim 61, wherein said method is implemented with one or more computer readable instructions embedded on a computer readable medium and configured to cause one or more computer processors to perform the steps of the method.